HP StorageWorks Fabric OS 5.3.2b release notes

Part number: 5697-0075
Thirteenth edition: July 2009

Legal and notice information

© Copyright 2009 Hewlett-Packard Development Company, L.P.

© Copyright 2009 Brocade Communications Systems, Incorporated

Version

5.3.2b

Effective date

July 2009

Description

Fabric OS 5.3.2b is a firmware release that contains fixes since the release of Fabric OS 5.3.2. There is no new device support added with this release for HP StorageWorks platforms.

Update recommendations

HP supports Fabric OS 5.3.2b on the SAN Switch 2/8v, SAN Switch 2/16V, SAN Switch 2/32, and SAN Switch 2/128 switches only. This release is not supported by HP on 4–GB or 8–GB switches.

NOTE:

If you are upgrading from Fabric OS 5.1.x with switches running 2.6.x in the fabric, upgrading to 5.3.2 is not supported unless 2.6.x switches are separated by a router.

Supersedes

Fabric OS 5.3.2 released January 2009.

Supported product models

- HP StorageWorks SAN Switch 2/8V (Brocade 3250)
- HP StorageWorks SAN Switch 2/16V (Brocade 3850)
- HP StorageWorks SAN Switch 2/32 (Brocade 3900)
- HP StorageWorks SAN Director 2/128 (Brocade 24000 Director)

Unsupported product models

Any switch not listed in Supported product models is not supported with Fabric OS 5.3.2b.

Devices supported

For a list of supported devices, see the HP website: http://www.hp.com/go/san.

Operating systems

For a list of operating systems, see the HP website: http://www.hp.com/go/san.

New features in Fabric OS 5.3.0

This section lists Fabric OS 5.3.0 added features and improvements:

NOTE:

The Fabric OS 5.3.2b firmware release contains the same features introduced in Fabric OS 5.3.0. However, given that 5.3.2b is supported only on 2–Gb switches, many of these listed 5.3.0 features, are not applicable to those switches.

- IPv6 support for the management ports
- Firmware download enhancements:
  - Support for Secure Copy (SCP)
  - Support for passive FTP
- iSCSI Blade–FC4–16IP enhancements:
  - Support for iSCSI redirection
  - Support for CHAP binding
  - Support for LUN delete from a virtual target
- Access Gateway (AG) mode support on the HP StorageWorks 4/16 SAN Switch (not supported on the 4/8 SAN Switch)
- Access Gateway enhancements:
  - WebTools support
  - Fabric Manager support
  - NPIV on F_Ports
- Fibre Channel Routing (FCR) enhancements
- IP broadcast zone support
- IP over FC also via FCR
- IP filter support (formerly MAC and Management port ACLs in Secure Fabric OS [SFOS])
- Support for FCS with base Fabric OS (formerly in SFOS)
- Support for multiple NTP servers
- Port mirrorinf for HP StorageWorks 4/32B SAN Switch
- Security enhancements
  - Support for security admin role
  - Support for account lockout for admin role
  - Support for strong password policies preventing repeat or sequence characters
  - P-EAP/MS-CHAPv2 support for RADIUS
- FCIP
  - Support for Fast Write and Tape Pipelining over secure tunnels (not supported by HP at the time of the release of this document)
  - Differentiated Services Code Point (DSCP) markings

- New Fast Write feature
- New SNMP features:
  - SNMP AD/RBAC support
  - 3DES and AES privacy protocol support
  - FCIP MIB
  - IPv6 trap destination
  - IPv6 SNMP ACL entries

Reliability, Availability, Serviceability (RAS)

The RASLog is modified to support IPv6. RAS will also obsolete `traceftp` and `savecore CLI` and add its functionality to `supportsave` and `supportftp`.

Management

Fabric OS 5.3.0 added a new user role: `secAdmin` or Security Administrator. This role maintains security administration, including logging and auditing. The addition of the `secAdmin` role allows users to isolate security management from complete Administrator management.

Security

Secure Fabric OS is no longer sold as an option, but integrated into Fabric OS 5.3.0 and later.

IMPORTANT:

Fabric OS 5.3.0 is the last major release that is compatible with SFOS.

Fabric OS 5.3.0 integrated the following new features:

- FICON cascading no longer requires SFOS.
- MAC policies have been replaced by IP filters, allowing configuration of acceptable IP addresses and ranges that may gain management access to the switch.
- Protected-Extensible Authentication Protocol (P-EAP with MS-CHAP-v2) support for RADIUS.
- DH-CHAP now supported for authentication of HBAs and end-devices in addition to switches.
- Additional password security options.
- Lockout of admin users that fail authorization.
- Flexible E_Port authentication settings, allowing better interoperability options for fabrics with varying levels of support. Certificate authentication is now optional.
- Auditing of authorization attempts.

New WebTools features in Fabric OS 5.3.0

This section describes the new WebTools features.

NOTE:

Some of the WebTools features are not applicable to this firmware release. Fabric OS 5.3.2b is supported on 2–Gb switch models only.

- Usability enhancements
  - Web-started GUI
  - Revamped Switch Explorer
  - Single-signed application
  - Common GUI components with new search and export capabilities
  - Advanced versus Basic views in Switch and Port Admin modules
  - Progress bars and other window-handling improvements
- Access Gateway enhancements
  - Full configuration of Access Gateway parameters, such as port mapping, Failover, and Failback policies
  - Tabular display of port mapping, port settings, port status, and world wide name (WWN) of attached devices
- iSCSI setup wizard for improved usability
- IPv6 support
- Support for Security Admin role, P-EAP protocol
- WTEZ Switch Setup enhancements
- Passive FCS support (enforcement but no configuration)
- IP filtering
- FC Fast Write support

Prerequisites

Table 1 summarizes the current Fabric OS firmware versions. HP recommends using the latest supported firmware versions to get the greatest benefit from the SAN.

For a list of retired products, see the HP website: http://www.hp.com.

IMPORTANT:

The Fabric OS versions listed in the **Earliest compatible version** column are the earliest versions supported by HP at the time of the 5.3.2b release.

Table 1 Supported Fabric OS versions

Model	Earliest compatible version	Recommended version

HP StorageWorks 1–Gb Switch	Not supported; end of support December 2007	
HP StorageWorks SAN Switch 2/8 EL HP StorageWorks SAN Switch 2/16 MSA SAN Switch 2/8	3.2.1b	3.2.1c
HP StorageWorks Core Switch 2/64 HP StorageWorks SAN Director 2/128 in Chassis (config modes 3 and 4 only)	5.0.5e	5.0.5f
HP StorageWorks SAN Switch 2/8V HP StorageWorks SAN Switch 2/16V HP StorageWorks SAN Switch 2/32 HP StorageWorks SAN Director 2/128	5.3.1b	5.3.2b
HP StorageWorks 4/256 SAN Director HP StorageWorks 4/8 SAN Switch HP StorageWorks 4/16 SAN Switch HP StorageWorks 4/64 SAN Switch HP StorageWorks B-series MP Router Blade (FR4-18i) HP StorageWorks 16 Port 4Gb Blade (FC4-16) HP StorageWorks 32 Port 4Gb Blade (FC4-32) HP StorageWorks 400 MP Router HP StorageWorks 4/32 SAN Switch	6.1.0d	6.2.0g
Brocade 4Gb SAN Switch for HP p-Class BladeSystem Brocade 4Gb SAN Switch for HP c-Class BladeSystem	6.1.0d	6.2.0g
HP StorageWorks 48 Port 4Gb Blade (FC4-48)	6.1.0d	6.2.0g
HP StorageWorks B-series iSCSI Director Blade (FC4-16IP)	6.1.0d	6.2.0g
HP StorageWorks 4/32B SAN Switch	6.1.0d	6.2.0g
HP StorageWorks MP Router	XPath OS 7.4.x	XPath OS 7.4.1e
HP StorageWorks DC SAN Backbone Director	6.1.0d	6.2.0g
HP StorageWorks SAN Director 16 Port 8Gb FC Blade (FC8-16)	6.1.0d	6.2.0g
HP StorageWorks SAN Director 32 Port 8Gb FC Blade (FC8-32)	6.1.0d	6.2.0g
HP StorageWorks SAN Director 48 Port 8Gb FC Blade (FC8-48)	6.1.0d	6.2.0g

HP StorageWorks SAN Director 6 Port 10Gb ISL Blade (FC10-6)	6.1.0d	6.2.0g
HP StorageWorks Fabric Manager Software	5.2.0a	5.5
HP StorageWorks B-series Data Center Fabric Manager Enterprise Software	10.0.2	10.1.4

NOTE:

The B-series MP Router Blade (for use with the 4/256 SAN Director only) must run Fabric OS 5.1.0d or later. The Core Switch 2/64 does not support the B-series MP Router Blade.

Firmware upgrade instructions

To access the latest Fabric OS 5.3.2b firmware, configuration files, and MIB files, see the HP website: http://www.hp.com/support/downloads and follow these steps.

1. Under Storage, select **Storage Networking**.
2. Select the link for the appropriate switch.
3. Select your product, and then select **Cross operating system (BIOS, Firmware, Diagnostics, etc.)**.
4. Under Firmware, select **v5.x Firmware for HP StorageWorks B-Series Fibre Channel Switches** for version 5.3.2b, and then select **Download**.

CAUTION:

Install port blades like the FC4-48 only after upgrading to Fabric OS 5.2.0a or later.

HP does not support upgrading directly from more than two previous releases. For example, upgrading from Fabric OS 5.1.x to 5.3.2b is supported, but upgrading from Fabric OS 5.0.x or a previous release directly to 5.3.2b is not.

Upgrading a switch from Fabric OS 5.0.x or a previous release to 5.3.2b requires a two-step process: first upgrade to Fabric OS 5.1.x or 5.2.x, and then upgrade to 5.3.2b.

The following conditions must be met before upgrading to Fabric OS 5.3.2b:

- Device-based routing must not be in use, otherwise the upgrade will fail. You can use the `aptpolicy` command to verify the routing policy.
- Chassis configuration options 3 and 4 are no longer supported for the 4/256 SAN Director.
- Fabric OS 5.1.1 supports a maximum MTU value of 2284. However, Fabric OS 5.2.1x and 5.3x support an MTU value of up to 2348. Before downgrading to Fabric OS to 5.1.1, you must change the MTU size so that it is less than or equal to 2284.

  If the configuration of the target unit has an MTU value that is greater than 2284, the FCIP tunnels will not go online after the firmware downgrade.

△ CAUTION:

If the 4/256 SAN Director integrates the FC4-48 Blade or any new software features in Fabric OS 5.2.0a (such as FCR trunking) you cannot downgrade to a Fabric OS version earlier than Fabric OS 5.2.0a. If you want to do so, you must (a) remove these features, (b) physically remove the FC4–48 Blade, and then (c) downgrade the firmware.

- For any other new software features or increased scalability limits supported by Fabric OS 5.3.x, the downgrade will be disruptive and will require a cold reboot.
- A Fabric OS 5.3.x configuration file cannot be used on the same switch after the switch has been downgraded to firmware version 5.1.x or 5.2.x.
- When you downgrade to Fabric OS 5.0.x, you must also remove additional 5.1.x features and any installed B-series MP Router blades.

Important notes

Table 2 provides important information about to this release.

Table 2 Important release information

Topic	Description
`ipfilter` command	Starting with Fabric OS version 5.3.0, you can use the `ipfilter` command to block unauthorized Telnet access. The option to disable Telnet using the `configure` command is no longer available. Use the following command to create a policy to block Telnet access to any station: `ipfilter --create blockTelnet -type ipv4 ipfilter --addrule blockTelnet -sip any -dp 23 -proto tcp -act deny ipfilter --activate blockTelnet` Use the following command to restore default policies for IPv4: `ipfilter --activate default_ipv4 --` See the *Fabric OS 5.3.0 command reference guide* for more information on the `ipfilter` command.
PKI certification	If you have purchased and installed the Secure Fabric OS option, go to the following HP website for information on obtaining a PKI certificate: http:// www.hp.com/storage/go/secureos.
FICON support	With release 5.2.0 and later, the Switch Connection Control high integrity requirement for cascading FICON is available in the standard base Fabric OS. End users can now deploy new cascade FICON Directors without purchasing a separate Secure Fabric OS license. To add a new FICON Director into existing cascaded configurations already running Secured Fabric OS, HP recommends that users continue to deploy Secure Fabric OS on the new FICON Director instead of migrating to FOS ACL configuration. NOTE: The FC4-48 port Blade is not supported to connect to System z environments via FICON channels or via FCP zLinux on System z. To attach the Director to the System z environment, use an FC4-16 or FC4-32 Fibre Channel port Blade.

Diagnostics backport test	Backport tests may be run only in the following configurations: • A pure SAN Director 2/128 (only CP2 and FC-16 blades) • A SAN Director 2/128 with no FC4-16 blades installed, using Option 5 Do not run backport tests in any configuration other than the two listed above; use the minicycle test instead.
Diagnostics spinsilk test	The following configurations will pass the spinsilk test: • A pure SAN Director 2/128 (only CP2 and FC-16 blades) • A pure 4/256 SAN Director, Option 5 • A pure 4/256 SAN Director, Option 5 (with FC4-16 blades) The following configurations will fail the spinsilk test; use the minicycle test instead: • A mixed SAN Director 2/128 (with either CP4 or FC4-16 blades) • A pure 4/256 SAN Director, Option 1 (a pure 4/256 SAN Director refers to a Director with CP4 and FC4-16 blades only)
Firmware up-grade/downgrade	When upgrading from Fabric OS 5.1.x to 5.2.x or 5.3.x, if two or more interfabric links (IFLs) connect to an edge fabric, one IFL will stay online and the other IFLs will go online and offline. This causes a temporary traffic disruption going from multiple IFLs to one IFL and then back to multiple IFLs. This is due to the new front domain consolidation feature in Fabric OS 5.2.0, where the IFLs connected to the same edge fabric share the same front domain. When downgrading from Fabric OS 5.3.x or 5.2.x, FC traffic will be disrupted if there is front domain consolidation prior to the downgrade, even in the case of a single IFL. Upon firmware download the FC4-16IP Blade does not preserve disabled GE_Ports in disabled state. If you want to retain GE_Ports in a disabled state across firmware download, you must configure them as persistently disabled.
Fabric OS — CLI com-mands	Obsolete commands include `slotOff` and `slotOn`; use `slotPowerOff` and `slotPowerOn` instead. The `portLogPortShow` command is also obsolete. This release does not support underscore (_) as part of the name for `dd` and `ddset` in the `iscsicfg` command. When performing a `configdownload`, you may receive a message stating `configDownload not permitted`. This indicates that an invalid parameter was passed to the switch. The invalid parameter could be from a switch security policy, such as the password policy, or the NTP server address. This causes a partial configuration to be downloaded onto the switch. For example, when an NTP server address is invalid, `configdownload` fails and all data processed prior to the NTP server address data had already been saved in the switch and cannot be backed out. To fix the problem, correct the invalid parameter and reissue the `configdownload` command.
Distance mode	Distance setting is not persistent. After a configuration uploads and downloads, distance settings reset and the desired distance is shown as 0.

FC Routing	If an HP StorageWorks MP Router is present in the backbone fabric, the command `fcrDisable` may take up to 8 minutes to complete. If the MP Router is replaced by a B-series MP Router Blade (FR4-18i) or an HP StorageWorks 400 MP Router, the command completes immediately. EX_Port trunking is not enabled by default. FCR switch does not support an edge fabric with one McDATA switch set to never principal. The EX_Port connected to that edge fabric will not come up. FCR switch does not support edge fabrics that consist of McDATA switches with domain ID offset. The EX_Port connected to that edge fabric may fail the RDI process and will not come up. EX_Ports come up disabled (failed to initialize in time) if attached to a Native mode switch running EOS 9.x that has nondefault DID offset configured. Device discovery may fail when an HBA uses the GA_NXT name server query to discover devices through an FCR switch, since the query is mishandled by the FCR.
Security	Remove any password enforced expiration of `admin` or `root` accounts before downgrading firmware to 5.0.1 or earlier versions.
Diagnostics	All offline diagnostics commands should be used only when the switch is disabled. Installing new SFPs during POST may cause POST to fail. Install SFPs only when the switch is `online` or if the switch is powered off. When you use the diagnostic commands `systemVerification` and `diagSetBurnin`, the switch or Blade faults when the burn-in error log is full. Clear the burn-in log before running `systemVerification` or `diagSet- Burnin`. If the ISLs reside on the switch that are not used for routing because they have higher link costs, disable the links before running `spinfab`.
HA	If there is an already segmented port and backbone devices are exported to an edge fabric, a build fabric/fabric reconfiguration can occur after running `haFailover`. Ensure that no segmented port exists before upgrading firmware.
Fabric Merge	Do not try to merge fabrics with conflicting domain IDs over a VE_Port. Before merging two fabrics over FC-IP with VE_Ports at each end, HP recommends that all domain ID and zoning conflicts be resolved.
Scalability	Support for Default Zoning policies has been added to Fabric OS 5.1.0. Typically, when you issue the `cfgDisable` command in a large fabric with thousands of devices, the name server indicates to all hosts that they can communicate with each other. To ensure that all devices in a fabric do not see each other during a `cfgDisable` operation, you can activate a Default Zone with policy set to `no access`. If Default zoning policies show enabled, all `cfgEnable/disable` commands and zoning changes must be run from a switch in the fabric running Fabric OS 5.1.0/5.2.0a. In large fabrics with more than 1,000 ports, HP recommends that the MS Platform Database be disabled. The Platform DB must also be disabled before downgrading to earlier versions of Fabric OS. This can be done using the `msPLMgmtDeactivate` command.
FRU insertion	The `FW_FRU_INSERTED` message is displayed twice when a power supply FRU is inserted and powered on. There is no functional impact.
System boot	Not all Fabric OS services run when the prompt becomes available during boot up. Wait for all the services to come up before using the switch or performing zoning actions.

Performance monitoring	If the user tries to save more than 512 monitors using the `perfCfgSave` command, some of the monitors may be lost.
Management — Proxy switches	If you using a Fabric OS 4.x switch as an API or SMI-S proxy to manage a 5.1.0 switch, you must be running Fabric OS 4.4.0d.
FCIP	Frame drops observed on FCIP slow links: • The frame drops occur when the FCIP tunnel bandwidth is set to 10 Base-T (10 Mb/s), E1 (1.048 Mb/s), or T1 (1.544 Mb/s). • With E1 or T1, frames drop even without an impaired link. • With 10 Base-T, frame drops may be observed when a low impairment is put to the link. The `portperfshow` command indicated incorrect (smaller) bidirectional throughput on the FCIP tunnel when Fast Write/Tape Pipelining is enabled. Fast Write/Tape Pipelining did not inform user when it failed due to multiple equal paths configured on 2 GbE ports. Backup jobs initiated from the Symantec BackupExec application slowed noticeably after adding significant I/O traffic from regular hosts and targets to the FCIP tunnel. A port-based routing policy must be used for Tape devices.
`portcfgdefault` command function change for the Brocade 4Gb SAN Switch for HP c-Class BladeSystem	Beginning with Fabric OS 5.2.1b, the `portcfgdefault` command now resets the configuration to HP factory default port settings.
Broadcast Zones	In Fabric OS 5.3.0 and later, a zone with the name broadcast (case-sensitive) is a special zone for setting up recipients of broadcast packets. In Fabric OS versions earlier than 5.3.0, a zone named *broadcast* does not have special significance. Therefore, you must make sure that if a broadcast zone is configured, the active and standby CPs use the same Fabric OS version. Otherwise, an HA failover might change the zone configuration.
Faulty SFPs	An external port with a faulty SFP will be disabled, then enabled once a good SFP is inserted. However, the port will still show as faulty even though it is healthy. To get the correct healthy indication, after enabling the port with the good SFP, remove and reinsert it and the port will then show as healthy.
FC Fast Write	Note the following important information when using FC Fast Write: • Only WWN zone (including normal zone and FC Fast Write zone) is supported on FC Fast Write enabled port. • Only single device loop port is supported. • NPIV (Access Gateway, for example) port is not supported. • FCR backbone devices are not supported. That is FC Fast Write should not be enabled on backbone devices. • FCR edge to edge support is limited by all the target devices on given edge fabric that host talks to should be connected to a 400 MP Router or B-series MP Router Blade in FC Fast Write mode. FC Fast Write should not be enabled on ports when testing the remote mirror application. • When a very high volume of traffic is being sent by host, FC Fast Write I/Os may time out and frame may be dropped. • Within the context of FC Fast Write, L_Port is not supported in Fabric OS 5.3.0 and later.

WebTools	When the regional language is set to anything other than English, Brazilian Portuguese, French, German, Italian, Japanese, Korean, Traditional Chinese, Simplified Chinese or Spanish, WebTools may not finish loading when connecting to a switch running FOS 5.3.0, 5.3.0a or 5.3.0b. The Switch Explorer progress bar hangs while initializing switch details. This problem is overcome by changing the regional settings for the operating system to English and reloading WebTools or by upgrading to 5.3.0c or later.

Additional Fabric OS 5.3.0 enhancements

Additional Fabric OS 5.3.0 enhancements include:

- New Fabric OS commands to rename an alias, a zone, and a zone configuration. `Zone –copy` copies the zone object to a new zone object. `Zoneobjectrename` renames the zone object.
- Detection and handling of a corrupted zone configuration `[under /etc/fabos/zone*]` gracefully instead of rebooting. The switch also logs the error in RASLog.
- A new command that provides both the WWN and serial number of the switch. Added an `–sn` option to display the serial number. For example, `wwn –sn` returns both the WWN and serial number data.
- Additional information on a faulty port in Fabric Watch to aid in troubleshooting.
- The use of passive FTP to download firmware.
- Enabling the customer to specify a quality password policy that prevents the selection of passwords with consecutive, identical characters.
- Multiple NTP servers with the `tsclockserver` command for redundancy. For example, if one site NTP server fails (DR scenario), there is a backup that can be reached by the switches.
- Logging a RASLog message when a 2.x switch joins the fabric.
- HA failover and user notification on the 4/256 SAN Director when there is a failed Ethernet chip (Oscillator chip).

Additional WebTools 5.3.0 enhancements

Additional WebTools 5.3.0 enhancements include:

- Individual error counters for FC ports from Port admin.
- SFP TX/RX power information in DB level from Port admin from WebTools.
- Clear Counter feature to reset all counters.
- Ability to clear 400 MP Router or B-series MP Router Blade GE port error counters using `portStatsClear` CLI command.

Fabric OS 5.3.1 fixes

Table 3 lists defects closed in the Fabric OS 5.3.1 firmware release.

Table 3 Fabric OS 5.3.1 closed defects

Closed defect summary	Solution
Management Server Daemon (MSD) panic occurs on switch during fabric initialization. When fabric has not initialized its database during fabric initialization, MSD gets IP address of switches in fabric which could lead to memory corruption and cause MSD to panic.	Fixed in Fabric OS 5.3.1.

Backbone to edge traffic across FCIP links and ISLs may not be evenly distributed across all possible routes (edge to backbone and backbone to edge).	Fixed in Fabric OS 5.3.1.
When disabling an NPIV switch which has an Access Gateway connected to it, the F_Ports that failover to the other NPIV switch show as `No device found` when running `nszonemember` for these F_Ports.	Fixed in Fabric OS 5.3.1.
When `perfMonitorShow –class ISL 0` command is run, some switches give incorrect output as follows: `The number of destination domains monitored is set to zero.`	Fixed in Fabric OS 5.3.1.
Unexpected switch reboot may occur during `hafailover`. During an upgrade, rcsd may get into an infinite loop and block RCS from completing a sync dump, leaving RCS transaction hanging. Switch panic may occur and traffic may be interrupted.	Fixed in Fabric OS 5.3.1.
Flooding of an unknown interswitch FDMI command from non-Brocade switch causes daemon to be killed due to out of memory condition, causing the switch to crash.	Fixed in Fabric OS 5.3.1.
Linux kernel issue may occur on 2Gb switches running Fabric OS 5.3.0x caused by service daemon thread (`fwd, nsd, fabricd`) becoming unresponsive due to deadlock condition. This can trigger a panic, or `snmpd` hang.	Fixed in Fabric OS 5.3.1.
Fabric OS crash occasionally seen when Access Gateway enabled switch is rebooted with large number of Access Gateway devices in the fabric.	Fixed in Fabric OS 5.3.1.
During `fastwrite`, specific third party device drops a frame that is not 8 byte aligned.	Fixed in Fabric OS 5.3.1.
With 2–GB switches, `hafailover` under heavy load across ISLs, followed by `portdisable/portenable` of E-ports causes port blade fault with tx parity error (error 21).	Fixed in Fabric OS 5.3.1.
When PID-2 change occurs, WebTools incorrectly translates the PID format in the NameServer and displays an incorrect account of the area/ports contained in a zone or alias member list. This can also happen when attempting to add to a zone or alias list, causing an incorrect physical port to be added.	Fixed in Fabric OS 5.3.1.
During stress test with 2Gb switch, when receive buffer overflow occurs, third party device port is stuck in offline state for more than 30 seconds. `Portdisable/portenable` will recover the port.	Fixed in Fabric OS 5.3.1.
Intermittent `supportsave` failure messages seen during `sup-portsave` loop.	Fixed in Fabric OS 5.3.1.
Traffic stops during FCIP testing with Tape Pipelining enabled, when host floods the switch with Name Server query. This occurs because the query response is not passed back to the host on the backbone switch through the FCR router.	Fixed in Fabric OS 5.3.1.
When executing `fastwrite` with Tape Pipelining with a slow responding tape device, the switch sent improper frame causing tape job to fail. Ultimately, this caused the initiator to lose access to the tape drive.	Fixed in Fabric OS 5.3.1.

When FICON host sends PLOGI directly to a device immediately after registering with the Management Server, PLOGI may be rejected because the routing tables have not been established.	Fixed in Fabric OS 5.3.1.
Incorrect GID FT response from Name Server caused host with multiple HBAs to log errors during HBA IOP reset. When host does its GID FT request, it gets a response for the other HBA though that HBA didn't register for FC4 type. Subsequent PLOGI, PRLI sequence to the non- FC4 type HBA is rejected and an error logged on the host.	Fixed in Fabric OS 5.3.1.
Automatic Fabric Configuration Server (FCS) policy distribution will not work properly on a future release with current Fabric OS 5.x in the fabric.	Fixed in Fabric OS 5.3.1.
Port `scn` removes logical paths from wrong port, resulting in some paths not coming online.	Fixed in Fabric OS 5.3.1.
If CALD restarts, it can no longer provide CAL cache data on EM, leading to possible SMI agent experiencing a reconnect issue.	Fixed in Fabric OS 5.3.1.
When a third-party system sends PLOGI/PRLI frames with its DID as a broadcast format, the 2/128 forwards the frame as a broadcast frame to all switch ports, causing other devices in the fabric to malfunction and overextend the switch CPU. This issue only affects 2/128.	Fixed in Fabric OS 5.3.1.
Occasional kernel panic occurs during reboot.	Fixed in Fabric OS 5.3.1.

Fabric OS 5.3.1a fixes

Table 4 lists defects closed in the Fabric OS 5.3.1a firmware release.

Table 4 Fabric OS 5.3.1a closed defects

Closed defect summary	Solution
F_Port link initialization failure caused by the switch not responding to NOS with OLS (continues to send idles).	Fixed in Fabric OS 5.3.1a.
When downgrading from 6.0.0x to Fabric OS 5.3.0c, then 5.2.1b, then 5.0.5a, the switch can get into an endless reboot causing file system errors to be reported.	Fixed in Fabric OS 5.3.1a If your switch is not upgraded to 5.3.1a, the workaround is to issue `firmwaredownload` with the -sf option: firmwaredownload `–sf` Use default answers so that `firmwaredownload` does not reboot after download, perform the following steps: `mount -oremount,ro /mntumount /mnt hareboot`
FR4-18i blade is faulted during operation with internal FCIP-5031 RASLog and external EM-1034 RASLog.	Fixed in Fabric OS 5.3.1a.
The `zoneadmin` feature in WebTools does not display the new ports after adding a new blade.	Fixed in Fabric OS 5.3.1a.

Only 1 FL port FLOGI is successful and second FL port FLOGI is disabled in a time interval. Even though FL port will be re-enabled after the short time interval, 3rd party failover application may fail.	Fixed in Fabric OS 5.3.1a.
When the proxy device projected to the backbone had a translate domain of greater than 0x20, router is not translating the ACC for a REC properly. Customer observes traffic interrupted and tape device fail.	Fixed in Fabric OS 5.3.1a.
When there is an application request GPPN on a device connected to multiple switches, customer might see continuous rtwr message on a pair of switches and directed at each other from msd: `[RTWR-1003],,, INFO, , msd0: RTWR retry 48 to domain 152, iu_data 1000000 RTWR Maxretries exhausted: 0x30, 0x8, 0x65, 0x0, 0x41d on multipath switches`. Potential for switch panic when memory is exhausted.	Fixed in Fabric OS 5.3.1a.

Fabric OS 5.3.1b fixes

Table 5 lists defects closed in the Fabric OS 5.3.1b firmware release.

Table 5 Fabric OS 5.3.1b closed defects

Closed defect summary	Solution
An `ipfilter --transabort` command running in one Telnet session can be aborted from another Telnet session.	Fixed in Fabric OS 5.3.1b.
Problems within an IP network could cause a switch running Fabric OS 5.3.x to panic.	Fixed in Fabric OS 5.3.1b. **Workaround:** Disable the clients trying to access evmd.
On the HP StorageWorks 2/128, when a specific 3rd party RAID system firmware is upgraded, the autonegotiate sequence fails, and the route to this device is lost.	Fixed in Fabric OS 5.3.1b. **Workaround:** Run `portdisable` and `portenable` to reset the port.
Switch did not send message to RASLog for `errdump` when status changed from `healthy` to `marginal` due to compact flash memory issue.	Fixed in Fabric OS 5.3.1b.

IMPORTANT:

All Fabric OS 5.2.3 closed defects as listed in the *HP StorageWorks Fabric OS 5.2.3 release notes* have been rolled into Fabric OS 5.3.2 firmware. However, note that these 5.2.3 closed defects have not been resolved in any 5.3.x release prior to 5.3.1 (specifically 5.3.0, 5.3.0a, 5.3.0b, 5.3.0c or 5.3.0d).

Fabric OS 5.3.2 fixes

Table 6 lists defects closed in the Fabric OS 5.3.2 firmware release.

Table 6 Fabric OS 5.3.2 closed defects

Closed defect summary	**Solution**

Zone transaction unable to commit and is rejected in a stable fabric.	Fixed in Fabric OS 5.3.2.
Switch panic can occur when the standby CP takes over and performs a cold recovery.	Fixed in Fabric OS 5.3.2.
Switch panic due to Out Of Memory kill caused by `msd` memory leak.	Fixed in Fabric OS 5.3.2.
User cannot access switch through network. If the contents of the `/etc/inetd. conf` file are modified, the file may be deleted the next time the switch software is upgraded.	Fixed in Fabric OS 5.3.2.
Switch hit a rolling reboot due to RTE DB inconsistency triggered by PCI scan failure on a failure blade during `hafailover`.	Fixed in Fabric OS 5.3.2.
User may be unable to connect to HP StorageWorks 4/32 SAN Switch from SMI Agent and see error related to limit of RPC handles open. `RPC` daemon indicates it has reached its limit of RPC handles, but `netstat` command does not show active sessions from the SMI Agent host.	Fixed in Fabric OS 5.3.2. **Workaround:** Reboot the switch.
WebTools zoning breaks when third party storage virtualization appliance changed to standby mode.	Fixed in Fabric OS 5.3.2.
Panic occurred during attempted multi-count write to compact flash.	Fixed in Fabric OS 5.3.2.
Invalid route table causes Class 3 Frame to drop. This happens on HP Storage- Works B-series Multi-protocol Router Blade/HP StorageWorks 400 Multi-protocol Router with EX_Port.	Fixed in Fabric OS 5.3.2.
`evmd` panic occurs when upgrading from Fabric OS 5.1.x to Fabric OS 5.3.x.	Fixed in Fabric OS 5.3.2. **Workaround:** Make sure both CPs are upgraded together.
Frame drop observed on 4–Gb and 8–Gb switches due to a time window when a port in a trunk goes offline and route is not properly recalculated.	Fixed in Fabric OS 5.3.2.
`Supportsave` during serviceability test detected memory corruption on FCRbased switch.	Fixed in Fabric OS 5.3.2.
CAL `EnumerateSelectedInstances` on Brocade_ISL is returning wrong `linkMembers` for McDATA switch.	Fixed in Fabric OS 5.3.2.
When default zoning is set to All Access, a potential race condition could cause the rejection of the NPIV PLOGI.	Fixed in Fabric OS 5.3.2.
`Auditcfg` not persistent through `hareboot`.	Fixed in Fabric OS 5.3.2.
Unable to run `portstatsclear` on a switch.	Fixed in Fabric OS 5.3.2. **Workaround:** Run `hareboot/hafailover`.
Port Peak Data Rate read from the SMI interface shows incorrect values that exceed the speed of the switch. Invalid Tx/Rx rate can be computed if a polling cycle takes place when a domain name has not been assigned.	Fixed in Fabric OS 5.3.2.
CALD memory leak seen when querying `EnumerateAssociatedInstanceKeys` on Phantom_switch to PhantomPort.	Fixed in Fabric OS 5.3.2.
The value of `sfpshow` no longer updates after `hafailover`.	Fixed in Fabric OS 5.3.2.

Too many FW-5002 messages causes a FFDC to be generated.	Fixed in Fabric OS 5.3.2.
`nsd` daemon is running out of memory.	Fixed in Fabric OS 5.3.2.
Switch experienced out-of-memory condition in `interopmode` with `nsd` being killed.	Fixed in Fabric OS 5.3.2.
WebTools does not work well in NAT environment.	Fixed in Fabric OS 5.3.2.
After security network scan of switch, IPADMd is no longer running.	Fixed in Fabric OS 5.3.2.
Speed negotiation fails on 4–Gb quadrate, long-wave 4–Km SFPs.	Fixed in Fabric OS 5.3.2. **Workaround:** Reset SFPs to avoid qualrate mode.
4–Gb switch running at fixed 2–Gb speed may not respond to FLOGI from HBA using auto-speed negotiation.	Fixed in Fabric OS 5.3.2.
WebTools zone admin alias displays duplicate PWWN on 48-port blade card.	Fixed in Fabric OS 5.3.2.
Fabric OS 5.3.0c WebTools zone sort by member of alias and member of zone is out of order.	Fixed in Fabric OS 5.3.2.

Fabric OS 5.3.2a fixes

Table 7 lists the defects in the Fabric OS 5.3.2a firmware release.

Table 7 Fabric OS 5.3.2a closed defects

Closed defect summary	Solution
A switch panic occurs due to a memory leak. This causes an `Out of memory` trigger during `hafailover`/`hareboot` when querying `connUnitPortFCId` in AG (Access Gateway) mode and when querying `FcFeModuleName`.	Fixed in Fabric OS 5.3.2a. Workaround prior to upgrade: Avoid this issue by not querying `connUnitPortFCId` in AG mode or `FcFeModuleName` MIB
If a second FDISC is received before the switch responds to the first FDISC between the same pair of devices, the Access Gateway daemon panics, triggering a reboot.	Fixed in Fabric OS 5.3.2a.
Access Gateway N_Port failover does not work if the HBA is brought online and the mapped N_Port is offline. In this case, the HBA is not sent to an available N_Port so that it can do a fabric login (FLOGI); instead, the HBA waits for its mapped N_Port to become active.	Fixed in Fabric OS 5.3.2a.

Fabric OS 5.3.2b fixes

Table 8 lists the defects in this Fabric OS 5.3.2b firmware release.

Table 8 Fabric OS 5.3.2b closed defects

Closed defect summary	Solution
The `agshow` command output not consistent across switches in the same fabric.	Fixed in Fabric OS 5.3.2b.
A switch panic can occur due to stack overflow on HP StorageWorks SAN Switch 2/32.	Fixed in Fabric OS 5.3.2b
SNMP does not return correct index values for the switch. Incorrect values are displayed for atTable, ipTable, and ipNetToMediaTable of MIB-2.	Fixed in Fabric OS 5.3.2b